POLÍTICAS E PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Fazem parte das Políticas e Procedimentos de Segurança da Informação da Neo Pack Indústria e Comércio Ltda, sem exclusão de outras práticas que se fizerem necessárias à proteção de dados e informações sob a guarda e sigilo da empresa, e vinculam diretoria, funcionários, técnico de TI, e demais contratados que, em virtude do contrato, venham a ter acesso e/ou trabalhem com esses dados e informações:

1. **Armazenamento de dados em servidor corporativo**
   Os dados devem ser armazenados todos no servidor principal da empresa, o qual é gerenciado em sala segura, com backups ativos semanais (em cloud e em disco rígido protegido com opção de criptografia). Dessa forma, sobrevindo a necessidade de qualquer equipamento ser retirado de seu local para conserto, ou outra ocorrência, os dados estarão seguros e disponíveis. É proibida a gravação de qualquer dado em unidade de memória (pen drives, HDs Externos e similares. Caso precise transferir dados internamente, utilize a pasta temporária no servidor (\\servidor\TMP). A transferência de dados para ambientes externos da empresa somente é permitida por setores autorizados.
2. **Definição de senha**
   Escolha senhas fortes, com 8 ou mais caracteres; o ideal é que tenha, no mínimo 14 caracteres. Combine letras, números e símbolos. Quanto maior a variedade de caracteres da senha, mais difícil será advinhá-la.
3. **Utilização de senha**
   É expressamente vedado o fornecimento de senha a funcionário da assistência técnica. Caso seja necessário, crie um usuário temporário em seu sistema para que o técnico possa utilizar.
4. **Alteração de senha**
   O ERP já está configurado para exigir troca de senha periódica de cada usuário. É imprescindível que troque suas demais senhas de acesso em um prazo a cada 90 dias.
5. **Antivírus e antispyware/malware**
   Deverão sempre ser utilizados bons antivírus e antispyware/malware. Eles ajudam bastante caso a tentativa em obter dados seja feita através de uma execução remota, ou seja, pela internet. Caso visualize mensagens no seu computador de expiração do anti-vírus, por favor informe imediatamente ao responsável de TI na empresa.
6. **Utilização de criptografia**
   Utilize criptografia nos diretórios onde há informações sensíveis.
7. **Acesso a sites**
   Somente acesse endereços de sites confiáveis, verifique se o link demonstrado é realmente o link que o endereço está sendo apontado. Ao entrar no site, verifique se todos os links funcionam corretamente. Muitos fraudadores lançam mão de páginas reais para fazer uma cópia e nessas páginas clonadas a maior parte dos links não funciona.
8. **Administração dos e-mails**
   Remova e-mails que chegam para você com propagandas não solicitadas, de modo a evitar alguma possível contaminação da máquina por vírus.
9. **Compras pela internet**
   Para maior segurança, fica proibida toda e qualquer compra pela internet que não seja relacionada com os interesses da empresa.
   Sobrevindo a necessidade, solicite ao superior responsável a escolha de lojas por ele conhecidas e que, tanto o ambiente físico quanto o virtual apresentam o mesmo nível de qualidade. Ao finalizar a compra, verifique se existe um cadeado no rodapé da página. Clique nesse cadeado para verificar a existência de um certificado digital válido. Esse certificado indica que a empresa onde você está fazendo a compra está seguindo os preceitos legais da internet no Brasil para compras online.
10. **Certifique-se**
    Certifique-se de que está trabalhando em um ambiente seguro sempre que for inserir informações do cartão de crédito ou dados de cunho pessoal, como CPF. Empresas de certificação digital possuem bandeiras disponíveis em links na página da compra. O consumidor deve clicar nesses links para verificar se estão abrindo corretamente. Assim, é possível ter mais garantia de que as informações que você disponibilizou serão protegidas e não serão utilizadas por outras pessoas.